DELPHI PRO

Diving Into Dark Pools

by Muhammad Yusuf

DEFI

Diving Into Dark Pools

Jun 7th, 2024 • 27 min read

Written by: **Muhammad Yusuf**

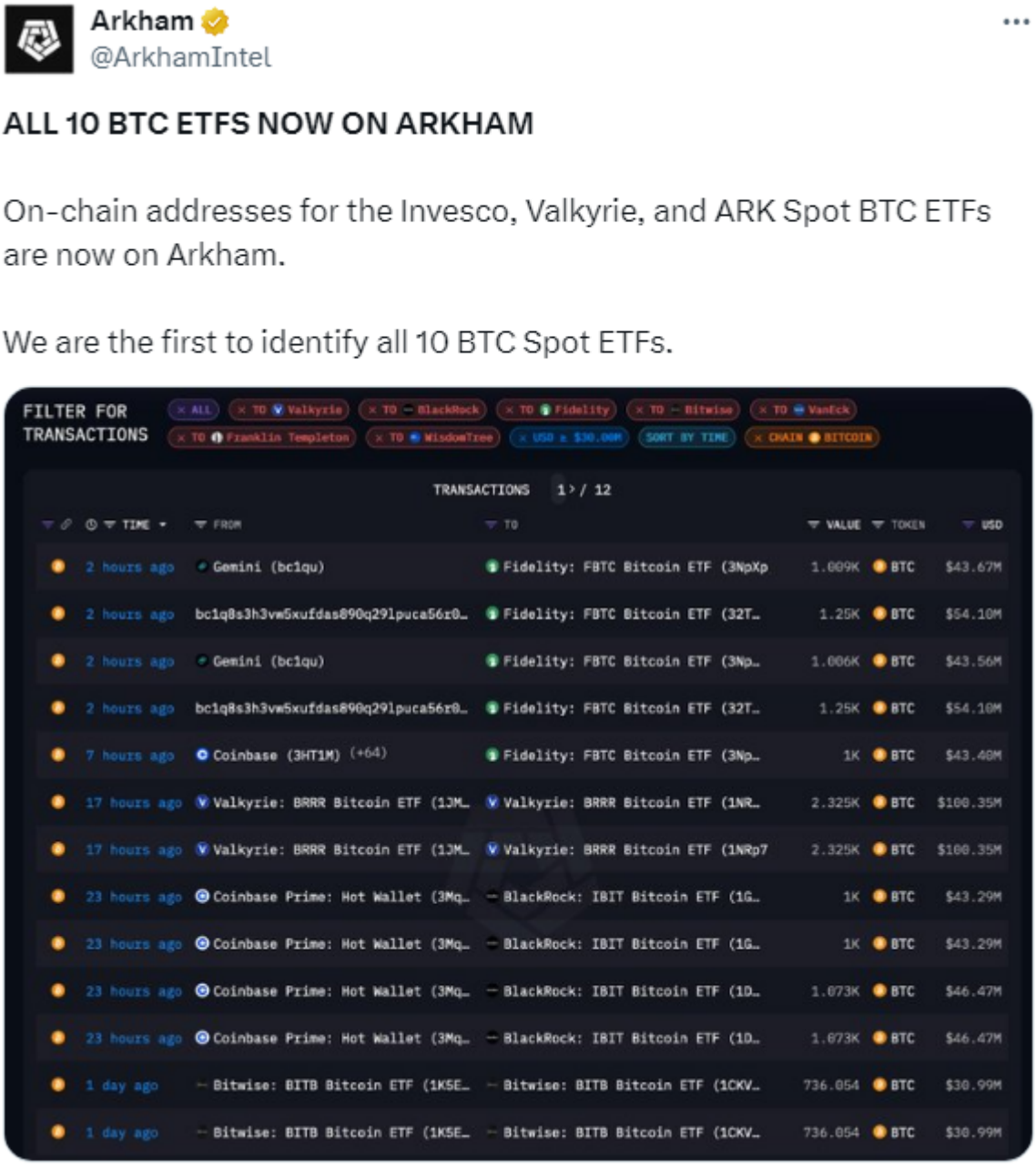
The author of this report may personally hold a material position in ETH. The author has not purchased or sold any token for which the author had material non-public information while researching or drafting this report. These disclosures are made consistent with Delphi's commitment to transparency and should not be misconstrued as a recommendation to purchase or sell any token, or to use any protocol. The contents of each of these reports reflect the opinions of the respective author of the given report and are presented for informational purposes only. Nothing contained in these reports is, and should not be construed to be, investment advice.

In addition to the disclosures provided for each report, our affiliated business, Delphi Ventures, may have investments in assets or protocols identified in this report. Please see here for Ventures' investment disclosures. These disclosures are solely the responsibility of Delphi Ventures.

Table of Contents

Dark Pools in the 60s 3
Mixers, Pools, and Everything in Between 5
Privacy Architecture 6
    Balance Models 6
    Proof Systems 9
Inner Working of Dark Pools 10
    Wallet Set-up 10
    Order Discovery & Matching 11
    Sourcing Liquidity 14
Business Models 15
MEV & Censorship Resistance 18
SEC's Good Book 19
Lingering Thoughts 20

With the BTC ETF out and running and ETH ETF making its way, the possibility of institutional crypto adoption is ever stronger. But there's a caveat. The extent of institutional crypto adoption may be hindered by the level of on-chain privacy they have. Arkham managed to track down the spot BTC ETF addresses of all 10 institutions.



https://x.com/ArkhamIntel/status/1752701573770477826

If we expect them to use the rest of what we have in Defi, that would necessitate some level of privacy on their part. For institutions, both from TradFi and crypto native, making large financial moves in the public has consequences. This is not

new to DeFi and has been a pain point in TradFi as well. This is where private financial products such as dark pools come into the picture.

Before diving into the inner workings of blockchain-based dark pools, let's set some context as to how dark pools came into existence, why they continue to operate, and to what degree they change the game.

Dark Pools in the 60s

In 1969, when computers were still large enough to take a room or two, and traders walked the trading floor shouting orders, institutional investors needed a better way to buy and sell their stocks without knocking off a domino effect in the market. Jerome Pustilnik pioneered electronic trading on Wall Street when he founded Instinet. Institutional investors could place orders, and Instinet would match and execute them. For something like Instinet to work, it would require significant volume on the demand and supply side of orders. So, what sweetened the deal for institutional investors? Confidentiality.

Instinet allowed the big guys to operate anonymously by concealing their identities and orders from other participants and the broader market. While this prevented their trades from affecting the market, it also meant a reduced risk of

being front-run by other traders.

As of 2022, over 60 dark pools were registered with the SEC. Some are exchange-operated, like the NYSE or NASDAQ; some are broker-dealer-operated, like MS Pool by Morgan Stanley and SigmaX by Goldman Sachs; and some are independently operated, like Liquidnet or MatchNow.

The issue with operator-run dark pools is that the operators potentially have more incentive to misbehave than to work in a compliant fashion. The equation is simple: **Profit from Corruption > Cost of Corruption.** Operators could get away with more profits than they would ever have to pay in penalties. In 2018, the SEC fined Citi Group $12Mn for misleading their investors about operating their dark pool while they leaked confidential order information to High-Frequency Traders who executed orders worth more than $ 9Bn against Citi's customers, profiting from them.

Traditional dark pool users run the risk of being played by their operators. It's a heavy price they've had to pay for participating in a broken trust model. Since 2011, dark pool operators have paid over $340 Mn in penalties to settle allegations. A relatively small price paid compared to the profits they may have accumulated. Blockchain-based dark pools try to abstract away the need to trust an operator who could behave maliciously. But there's a catch.

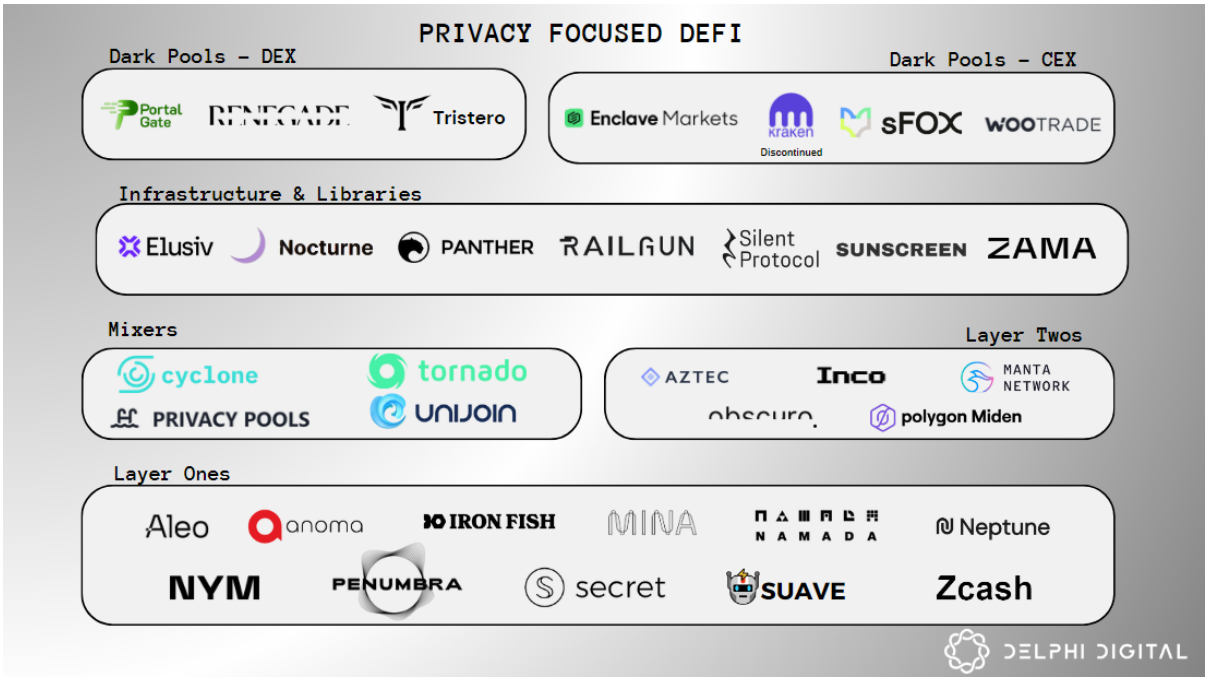
Mixers, Pools, and Everything in Between

Blockchains were initially designed to be fully transparent. While it promotes accountability, it is a double-edged sword. If you received a salary payment on-chain, anyone with your wallet address could see how much you were paid over the years and how much you would be paid in the future.

DEXs (Decentralized Exchanges) and wallets are subject to be tracked by wallet tracking and copy trading platforms which take it even further by allowing anons to snipe well-performing traders, complicating their trading strategies. Large orders also risk being front-run by searchers in public mempools.

Before we get into dark pools, let's distinguish between them and mixers. Mixers are a subset of dark pools. Mixers like Tornado Cash mix tokens to break links between wallets and assets to make it difficult to trace the source of funds. Dark pools, on the other hand, not only break links between wallets and tokens but also help users trade amongst each other without revealing any information about the other parties.

Now that we've looked into the origins and motivations behind traditional dark pools and distinguished a mixer from a dark pool, let's dive into blockchain-based dark pools that instill privacy in their base-level architecture with Balance models and PETs (Privacy Enhancing Technologies) such as Zero Knowledge, MPC, FHE and TEE.



The market map may not be inclusive of all privacy and privacy-focused DeFi companies

As of writing this, dark pools like Singularity, Renegade, and Tristero are under development.

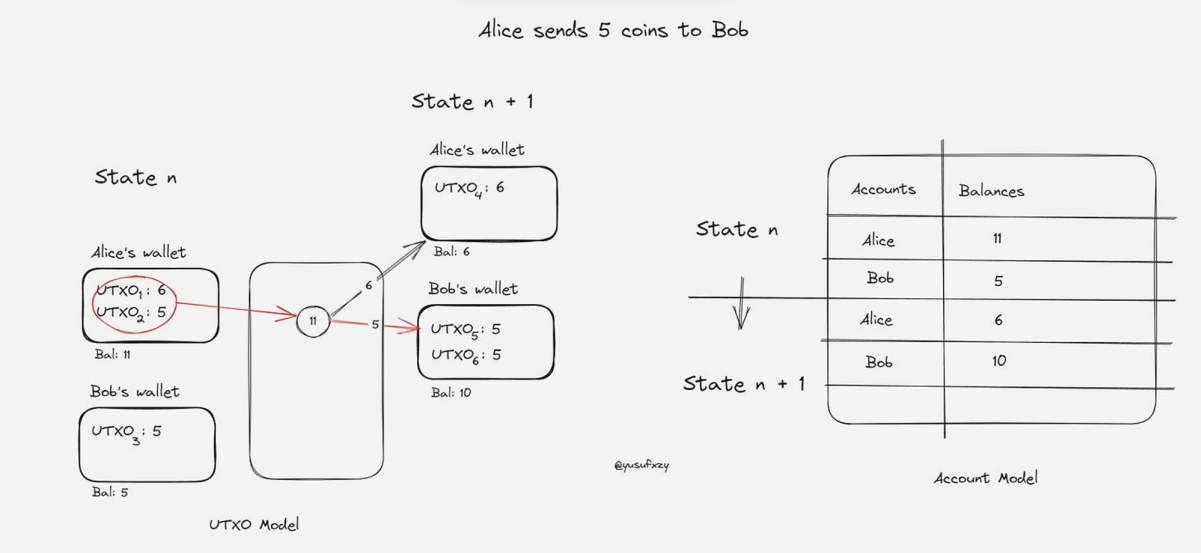
Privacy Architecture

Balance Models

Blockchains are state machines. The state is composed of accounts and transactions. As accounts transact, with every state transition, a new set of updates is added to the chain. The balances of the accounts are also updated. Balance Models are different ways in which a blockchain tracks and manages user account balances. Blockchains such as Ethereum, Solana, and Polygon utilize the Account model and Blockchains such as Bitcoin, Zcash, and Monero use the UTXO model. These models differ in how they manage and present the state of a blockchain.

The Account model, similar to a bank account, shows the current state as a set of addresses and their balances. Whenever you make a payment, you send the exact amount, no change is left over on either side, and no new balances are created. But the UTXO (Unspent Transaction Output) model isn't as straightforward. When you make a payment, your entire balance is transferred,

burning your existing balance. The remainder of what you own is added to a new balance. The UTXO model shows the current state as a graph of all the spent and unspent outputs of transactions.



To illustrate, consider this scenario,

Alice's wallet contains two UTXOs with 6 coins and 5 coins, while **Bob**'s wallet ****holds a single UTXO with 5 coins. When Alice sends 5 coins to Bob, she combines her two UTXOs into a single transaction, making it difficult for observers to figure out the source of the 5 coins she sent to Bob and what happens to the remaining balance in her UTXOs. This privacy-preserving mechanism effectively obscures the flow of funds and maintains the confidentiality of transaction participants.

A newly generated UTXO doesn't have a known owner and requires advanced chain analysis to be linked to a single user. With the account model, there is fungibility. It encourages address reuse and hence makes it easy to track history for a single user.

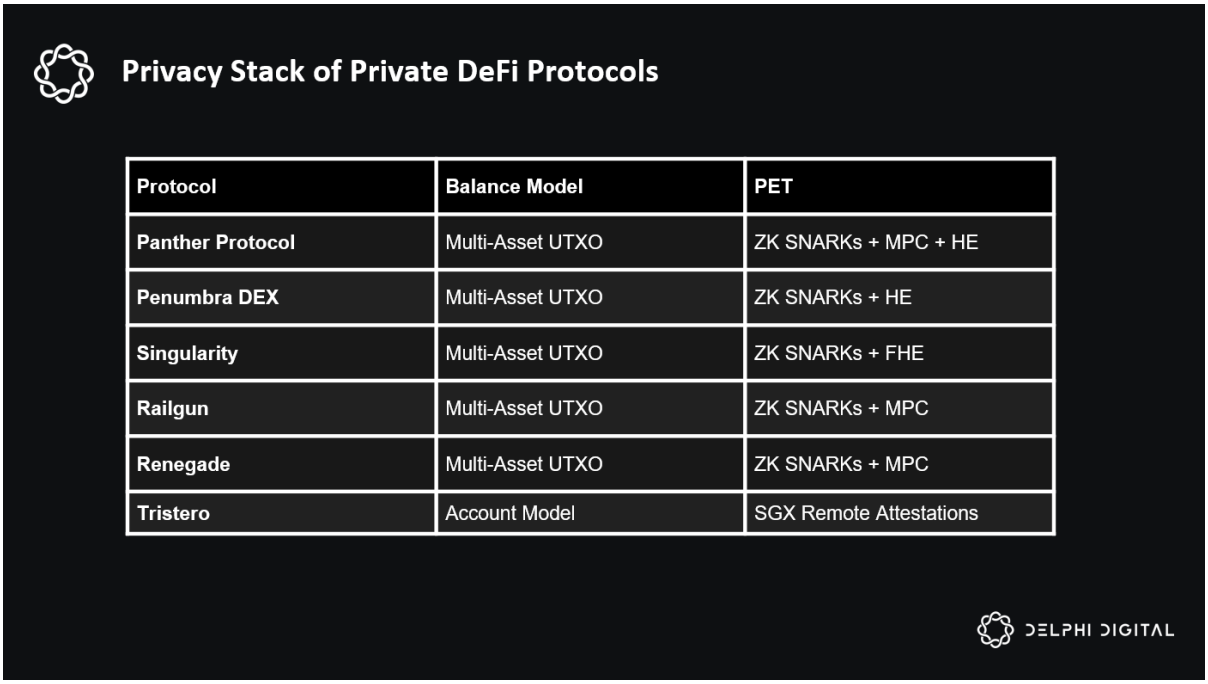
It is also quite difficult to double-spend with the UTXO model in place. Each UTXO has a unique nullifier derived through itself. When a transaction is being verified, i.e. when the UTXO is being spent, its nullifier is also spent. This prevents a transaction from being spent again.

Several versions of the UTXO model have been used across L1s and L2s focused on privacy. Aleo uses the Record model which is a variation of the UTXO model. Aztec and Polygon Miden use a hybrid of both UTXO and Account model.

The UTXO model used by Zcash heavily inspires the UTXO model used in dark pools. Individual protocols have modified it to support multiple assets and

accounts. Protocols like **Singularity, Penumbra, Railgun, and Renegade** use a note-based mechanism where each UTXO is a note. These notes, like a UTXO, contain information about the asset, order, and value, but are only visible to the owner/user. These notes are stored within Merkle trees that store the state of the chain called State Commitment Tree. These notes may be created as a result of internal transfers or settlements within the dark pool, or by a fee payment made to a relayer. Renegade uses enshrined MPC to match UTXOs (orders) and update private state. Multiple notes can be stored within a single note as well.

Tristero uses an account-based model similar to Ethereum. Trade orders in Tristero, are encrypted and delivered to a network of TEE nodes in the form of intents. Before delivery, these intents are "salted" (cryptographically adding randomness) to make it harder to guess the order input that would generate the SHA256 hash. These intents include information such as user address, order asset, and order quantity.



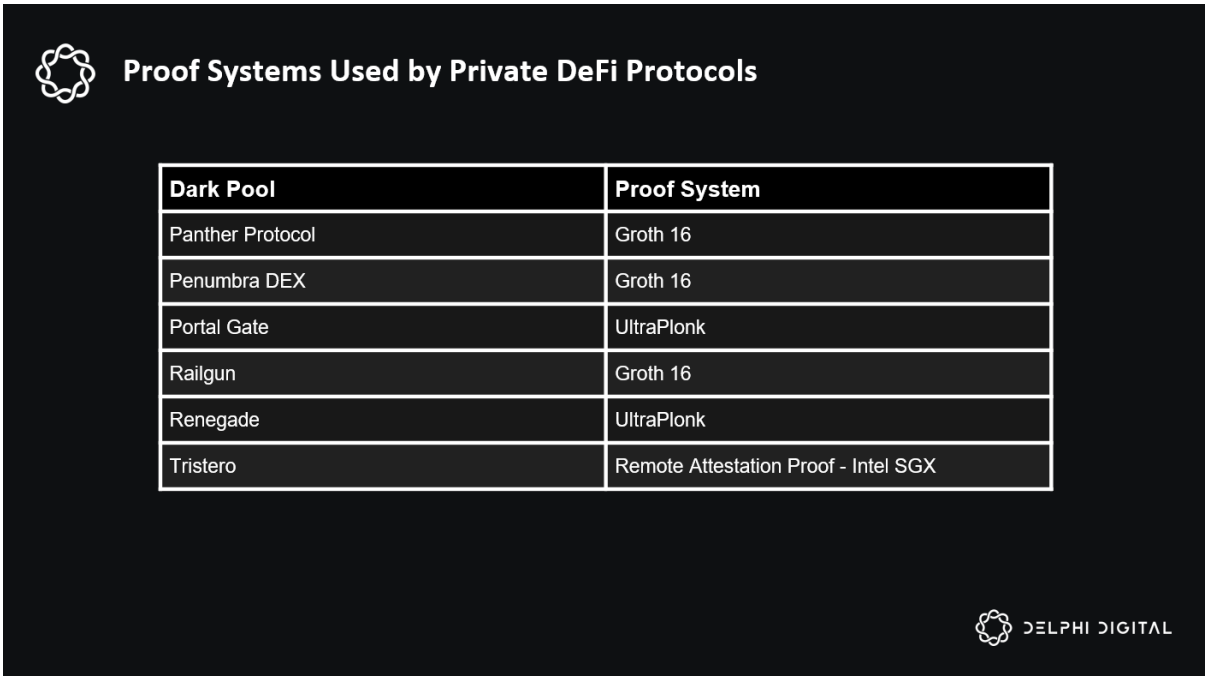
Protocol	Balance Model	PET
Panther Protocol	Multi-Asset UTXO	ZK SNARKs + MPC + HE
Penumbra DEX	Multi-Asset UTXO	ZK SNARKs + HE
Singularity	Multi-Asset UTXO	ZK SNARKs + FHE
Railgun	Multi-Asset UTXO	ZK SNARKs + MPC
Renegade	Multi-Asset UTXO	ZK SNARKs + MPC
Tristero	Account Model	SGX Remote Attestations

With **Panther Protocol** each asset or account is represented as a zAsset or a zNFT and the UTXO model operates through a Merkle tree called "Bus" that processes UTXOs in batches with up to 64 UTXOs in each batch, optimizing cost efficiency for users. "Bus operators" handle the processing, and users incentivize them with rewards denominated in $ZKP. When it comes to executing individual UTXOs, Panther has what's called a "Taxi" Merkle tree. To support multi-chain UTXOs, a "Ferry" Merkle Tree.

Proof Systems

This is where one of the primary PETs (Privacy Enhancing Technologies) comes into play. Zero Knowledge Proofs are used to prove the possession of correct information without revealing it. In the context of dark pools, ZKPs can be issued to prove that a user has sufficient funds and permissions to place orders and have them match and settle, all while keeping these particulars hidden from dark pool operators, fellow traders, and external third parties.

Proof systems are cryptographic constructs designed for generating these proofs. They come in various types, each producing proofs of different sizes, requiring varying timeframes, and consuming different computational resources for both generation and verification. Here, we will delve into two prominent proof systems: Groth16 and UltraPlonk, which have found applications in the dark pools we've discussed.



Panther, Penumbra, and Railgun leverage the Groth16 proof system to produce their proofs. Groth16 is known for generating proofs of a consistent size, making it a favored choice as proof size may have implications on transaction size, gas costs, and throughput. On the other hand, Singularity and Renegade utilize the UltraPlonk proof system.

Both Groth16 and UltraPlonK require a trusted set-up, where a group of trusted parties collaborate to establish a common set of parameters. These parameters are used to verify proofs in a way that the verifier need not trust the prover and the prover need not trust the verifier. It's crucial to note that a trusted setup

implies trust assumptions about the involved parties. Secure Multi-Party Computation can be used to safeguard against any single party gaining access to the underlying setup structure. Groth16 relies on inputs from multiple parties for its trusted setup, while UltraPlonk only requires the involvement of a single party.

With **Tristero**, each node runs inside an Intel SGX enclave, which runs a Trusted Execution Environment. These nodes handle sensitive trading operations, specifically managing order matching and maintaining the darkness of the order. To ensure that the dark pool is secure and not compromised, each node within Tristero must issue remote attestations. Remote attestations help verify the integrity of a node within the TEE network.

At start-up, when each node initializes its Intel SGX enclave, it generates a code and hash of all the data the enclave contains in a "report." This report is verified locally and then sent to another enclave that verifies and includes it in a "Quote." This quote is then sent to a third party, IAS (Intel Attestation Service), to verify that the node has not been tampered with. A token of this attestation is returned to the user, which proves authenticity.

Inner Working of Dark Pools

Let us now go through the inner workings of dark pools, how they preserve privacy while conducting trades, source liquidity, prevent MEV extraction, their nature of censorship resistance, and compliance in the following sections.

Wallet Set-up

In most cases, you will be required to create new, specialized wallets to interact with dark pools. Railgun has a third-party wallet provider called Railway Wallet that allows you to create an encrypted EOA that lets you hold a balance of shielded tokens/NFTs and also call any public smart contract you want privately through a Relay Adapt mechanism.

With Renegade, a wallet is the same as a UTXO that has private keys and can sign transactions. You will need to generate a new UTXO and commit to it using a ZK proof. This proof proves that the new UTXO is in fact new and that you have not already spent the funds that it contains. Most operations like depositing, placing orders, and trading will nullify that wallet, leading you to create a new one to

ensure no double spending occurs. The UX remains the same as any other Ethereum wallet.

To use Penumbra, you would create a new wallet as you would while first starting with any other cosmos chain. After which the wallet can be funded through another IBC transfer.

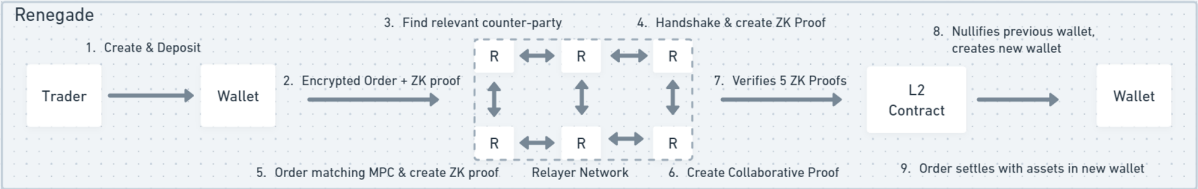
With Panther and Singularity, a KYC process is in place. An Ethereum wallet can be used but the connected wallet user must verify their passport to gain a credential to interact with the protocol. Business entities require a KYB where they share their business details. The verification is done off-chain with a registered compliance provider. These credentials expire periodically, after which the verification must be repeated.

Order Discovery & Matching

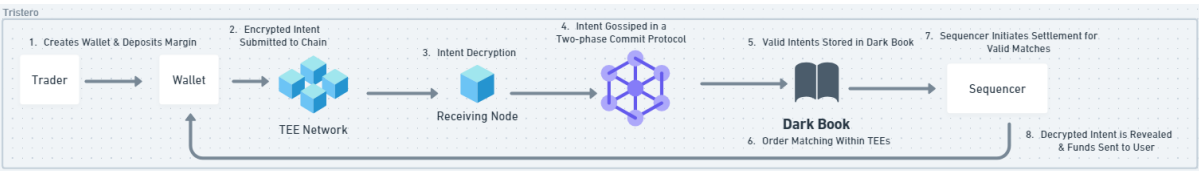
When it comes to order discovery and matching, general DEXs like Uniswap and Curve take an Automated Market Maker approach where orders are matched against a liquidity pool. This method is not the best choice for privacy because when orders are matched against a public liquidity pool, the order details are publicly visible on the blockchain. This is not ideal for traders dealing in large volumes as it may reveal their intentions to other players in the market who may take advantage of that information. Some dark pools that do end up matching against liquidity pools or using other external public contracts for order matching make use of relayers that act as a Chinese wall between traders whose privacy must be preserved and the external liquidity sources. We'll look into how dark pools source liquidity while maintaining privacy in the next section.

As for now, remember, traders have already deposited funds into their wallets in the dark pools. We will now go over what happens when an order is placed. Some dark pools take a Peer-to-Peer approach to order matching whereas some take a Peer-to-Pool approach using PETs like Zero-Knowledge or Multi-party Computation while their internal contracts interact with external public contracts. Taking the peer-to-peer approach or crossing orders between traders can help with better execution without slippage. Because if orders were matched with a liquidity pool, the price of the liquidity pool could change between the time the order is placed and when the order is executed. When orders are crossed between traders, the order will be executed on the agreed-upon price between them.

With Renegade, which takes a Peer-to-Peer approach, when a trader submits an order, they also choose a relayer who can do their bidding (matching orders) for a fee. The trader generates a ZK Proof called “VALID COMMITMENT” saying that they own their wallet and its orders. A “handshake” is then sent out to the network to match with handshakes of other traders. A handshake is essentially an immutable list containing the VALID COMMITMENT ZK Proof, hashed order details, a nullifier, and key pairs. When a trader’s handshake match is found with another trader’s handshake, they proceed with Multi-party Computation. Renegade uses collaborative ZK-SNARKs to prove that the trader’s orders truly match with that of the counterparty. This ensures that the order details are kept hidden from other parties while the order matching is being done. Once orders are matched with all the required proofs, a new wallet is created in which the swapped tokens are deposited after verifying that the wallet is indeed new to prevent double-spending. The UX remains the same as using any Ethereum wallet.

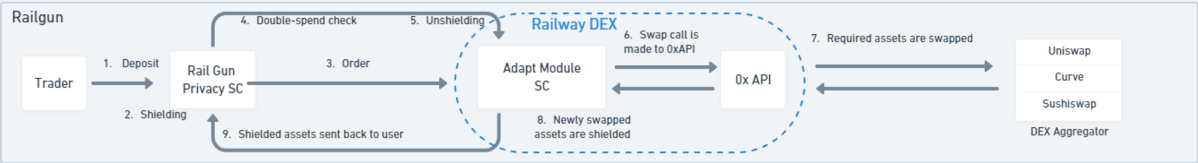


In Tristero, users submit encrypted orders to network nodes running in Trusted Execution Environments (TEEs). These orders are initially validated by the receiving node and then propagated to other nodes through a gossip protocol. The network ensures consensus on the order’s validity through a coordinated confirmation process. Valid orders are stored in a dark order book within the TEEs, where a matching engine identifies potential matches. Tristero’s order confirmation time is currently ~80ms, and order matching time is 100ms, performance numbers that are only achievable today through TEEs. When a match is found, nodes collaborate to stage and verify a transaction, which is then settled on Ethereum. While TEEs offer weaker privacy guarantees than other approaches, they also enable designs that offer better latency. Tristero’s design only requires that users trust Ethereum, as the commit reveal scheme prevents Tristero’s network from stealing user funds.

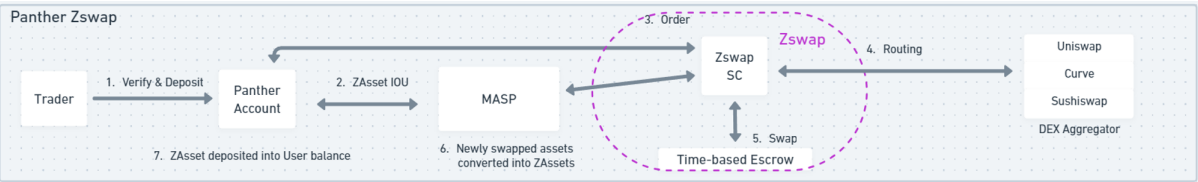


Railgun, when a trader places swap orders through Railgun, a smart contract called Adapt Module performs multiple actions, i.e. takes the trader’s specified private balance in his wallet that he wants to swap and unshields it. Adapt Module

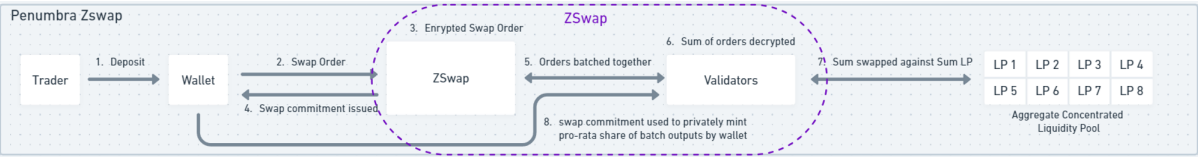
will also verify that the order (UTXO) has not been nullified/spent already. The 0x API then swaps the assets across aggregated DEX liquidity looking for the best rates. Adapt Module then shields the swapped assets back into the private balance, such that their activity or addresses are not revealed. This workflow can also be applied to other DeFi transaction types.



Panther Protocol also operates similarly wherein it uses a module called Zswap that connects Panther's MASP (Multi-Asset Shielded Pool) with other DeFi protocols. The MASP is less of a "pool" but more of a collection of "append-only" Merkle trees, where each leaf is a commitment to a UTXO representing an IOU of an asset deposited into the MASP. When a trader is creating an order, Zswap aggregates quotes from other DeFi protocols for the trader to choose from. Once an order is placed, Zswap creates an encrypted time-based escrow contract that can privately facilitate swaps between users without revealing any details. Once the assets are swapped, the user receives an IOU of the token in the form of a ZAsset (ZNFT) from Panther's MASP.

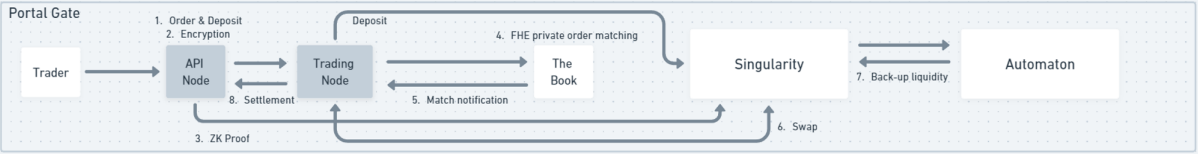


Penumbra's swap module is also called Zswap but it works quite differently. When a trader creates an order, the asset in the trader's private balance is burnt and the encrypted order values are sent to validators. A fee is also paid to process the order. A "swap" NFT is given to the user to keep a record of the event. The NFT is identified with a combination of various parameters, including the assets being traded, the fee, input amounts, and cryptographic keys. Validators aggregate order inputs from several traders into a single batch and then these inputs are executed against concentrated liquidity positions. Once executed, the outputs are delivered to the trader proportionate to each trader's input. In this case, individual data remains private but aggregate data is exposed when validators aggregate orders to execute against concentrated liquidity positions.



With Singularity, when a trader submits an order, an API node picks it up, encrypts it generates a ZK proof, and relays the order to the Book, which is a set of off-

chain nodes that collect orders and runs an order-matching algorithm inside an FHE (Fully-Homomorphically Encrypted) environment. This means that the encrypted orders need not be decrypted to be matched. Once orders are matched, the sum result of all the orders being matched is shown while no details of individual orders being matched are revealed. This again helps preserve privacy.



Sourcing Liquidity

Dark pools like Renegade, Tristero, Singularity operate by anonymously crossing buy and sell orders directly between users but it may not always be the case that liquidity on the other side of an order is available. With general DEXs, you are almost guaranteed liquidity for your orders, but you trade it off for privacy and price impact. Privacy, because anyone can have a look at what you are selling or buying. Price impact, because guaranteed liquidity comes with a premium that you end up paying for along with your order. With dark pools, the order information is kept hidden both before the trade and after it.

Renegade follows this design philosophy by matching order flow with counter-order flow without going through any intermediary liquidity providers. In cases where liquidity is lacking, a mechanism called “Indication of Interests” is in place where a trader can reveal certain details of their order to relayers that match orders. Details like price, size, asset, and order type are effectively proven through zero knowledge. If traders choose to reveal such details, other traders would be able to view these orders resting on the order book, potentially leading to these orders being executed faster.

Panther Protocol is not only a dark pool. It has a host of other DeFi activities that can be performed privately. A user starts by depositing into a Multi-Asset Shielded Pool representing deposited assets as a ZkAsset (ZkNFT). Essentially an IOU token, similar to that of the stETH you get when you stake Ethereum. Plug-ins called DeFi Adaptors connect the MASP with existing DeFi protocols privately. Zswap is an adaptor that connects the MASP with DEXs such as Uniswap, Quickswap, Curve, and more. Panther also has another module called ZTrade that matches user orders internally without using external liquidity.

Penumbra, like Panther or Railgun, is an avenue for several DeFi activities. Within

Penumbra, users end up creating their own little AMM when they start an LP position. So you have a collection of tens of thousands of concentrated liquidity positions created by users who set their own desired fees. This would fragment liquidity but Zswap / DEX Engine would consider and synthesize all of these individual liquidity positions into a single AMM. This would make it possible to route incoming trades across the entire liquidity graph.

Tristero will primarily match user order flow with counter-order flow like an orderbook, similar to Renegade. Liquidity will be bootstrapped in an old-school way by bringing on market makers.

With Singularity, an anonymous AMM-DEX, Automaton is used to facilitate liquidity as a backup to the Book, i.e. the relayer runs an order book used to cross users trades with each other. If and when the book fails to facilitate trades due to lack of liquidity, the orders are routed to Automaton. Liquidity will be bootstrapped at Automaton like any other AMM.

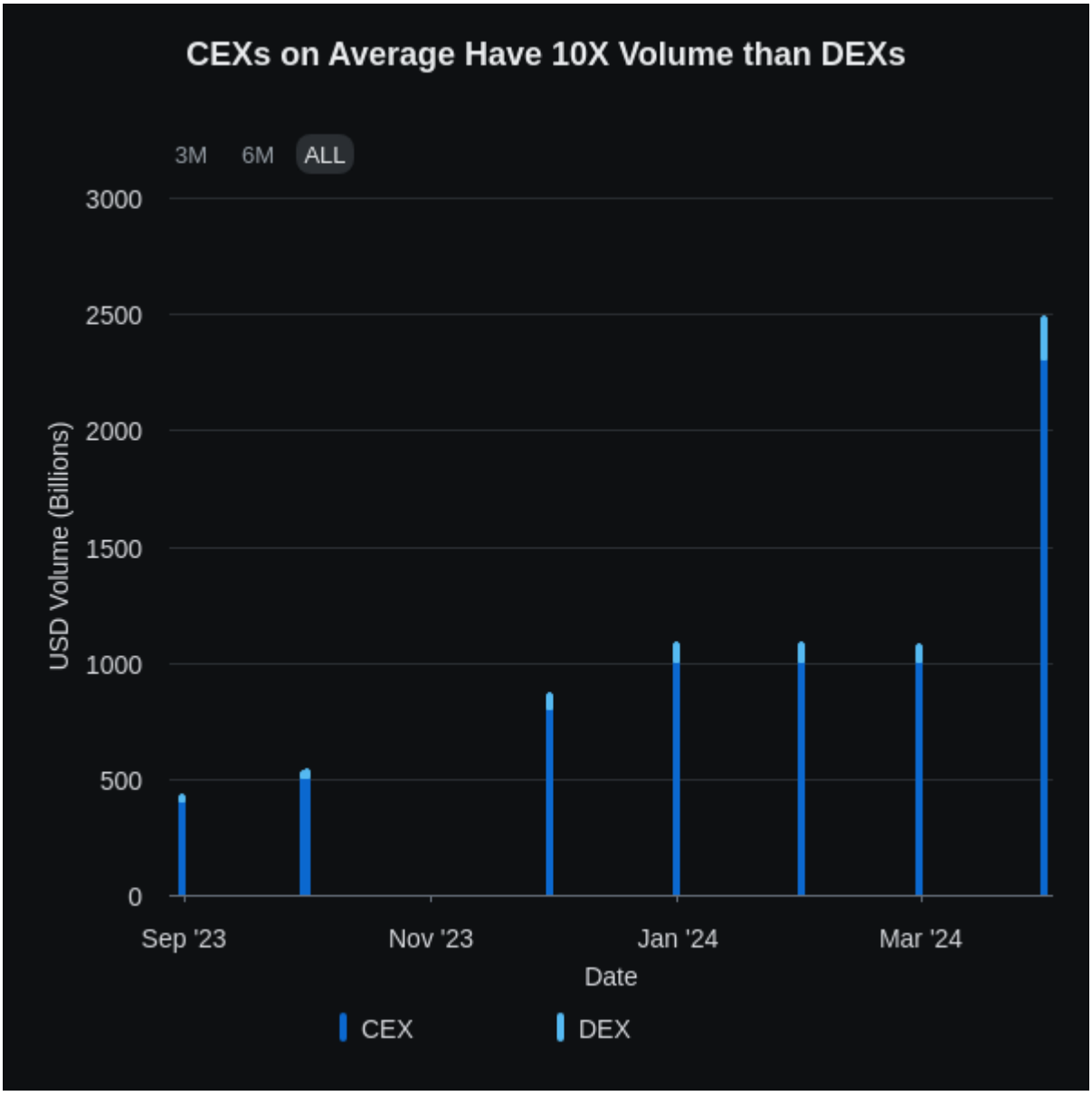
Railgun's Railway DEX uses the 0xAPI built by 0x. This means that orders out of the Railway DEX are routed to find the optimal price for execution across the 0xAPI DEX aggregator. Once a trade route is found, the wallet generates proof to use the funds in the trader's balance to swap and shield the incoming tokens from 0xAPI to the trader's balance.

Business Models

Tradfi dark pools are treated more or less like an elite club where the ones with a fat balance trade. They pay membership fees to the dark pool to be able to place orders anonymously and also to have relevant counter-order flow come in from the other side. Trading fees are generally lower than tradfi exchanges. Tradfi dark pools may also act as brokers where they buy securities from a seller at a lower price and then sell it to another buyer at a higher price.

Dark pools in crypto move away from this "operator" focused design to act more in the way of a "facilitator". They aim to generate revenue through two major components. Protocol fees on orders that are matched successfully and a portion of relayer fees paid by a trader to a relayer to handle transactions. A portion of the relayer fees could also go to the relay operator. Traders may also choose to run their own relayers for better privacy and to avoid paying relayer fees.

Decentralized dark pools in crypto may face a cold start problem. Unlike DEXs that trade against a liquidity pool, most dark pools have users trade against each other by matching buy and sell orders. It is crucial for such a system to have traders on both sides of the market placing orders. It is also important to note that dark pools in tradfi were hosted by multi-billion dollar banks like Goldman Sachs and exchanges like NYSE. This way, supplying order flow to their users would have been relatively easier. There are also standalone dark pools like Liquidnet who had estimated that they would require at least 100 buy-side firms to be live on their platform since day to reach critical mass but ended up launching with 38 firms. Liquidnet is now among the top 3 largest dark pools in the world.

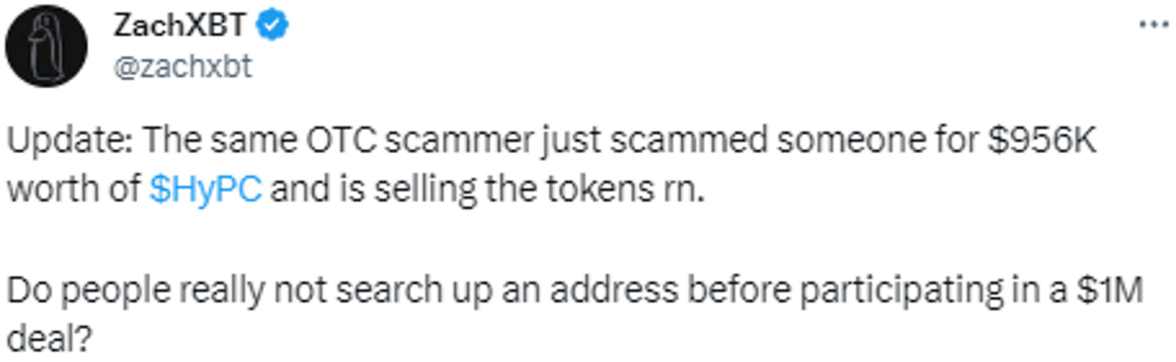


Centralized exchanges on average have 10x more volume than Decentralized exchanges given their wider user base drawn to better UX and compliance, which in turn increases supply to satisfy demand. Liquidity for OTC deals is relatively

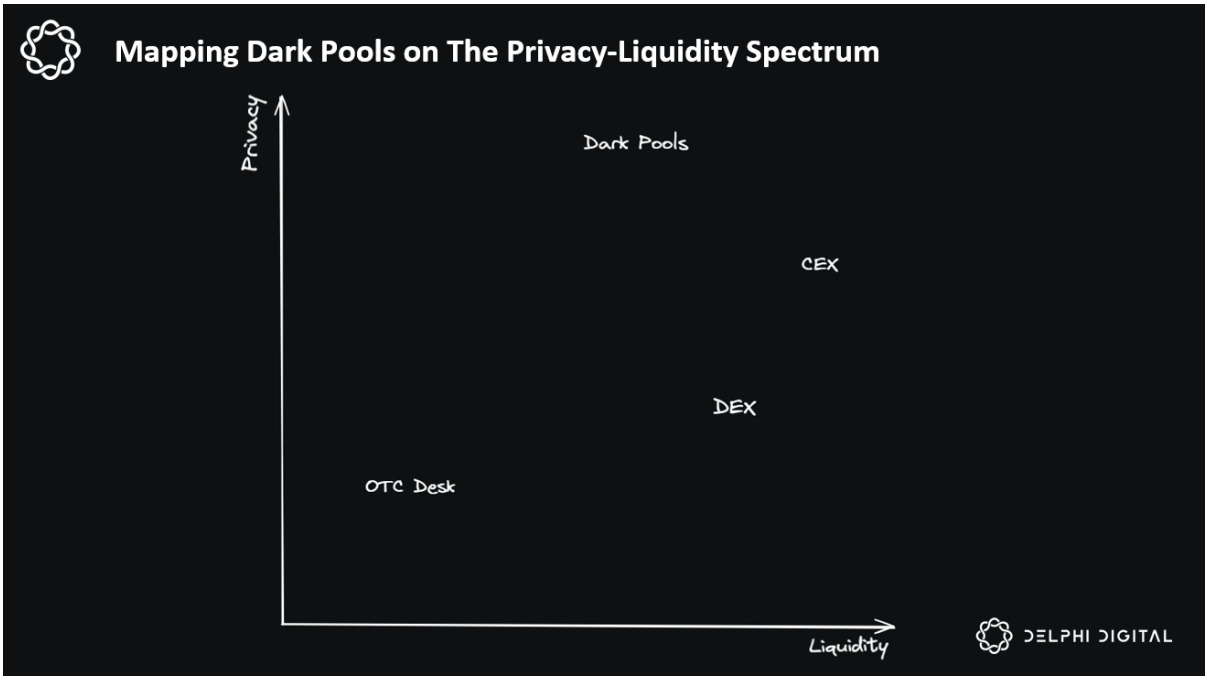
harder to come by.

Most OTC deals in crypto are facilitated through OTC desks and escrow smart contracts and even Telegram groups in several instances. And it's a shocker. People get scammed regularly. It is quite convenient for scammers to impersonate on Telegram, edit messages, and deal details. With dark pools, you may not be guaranteed immediate settlement for an illiquid token or an NFT but it ensures a greater level of security and privacy. With OTC deals happening over dark pools, customers of OTC desks would not have to pay a broker's fee either.

Source



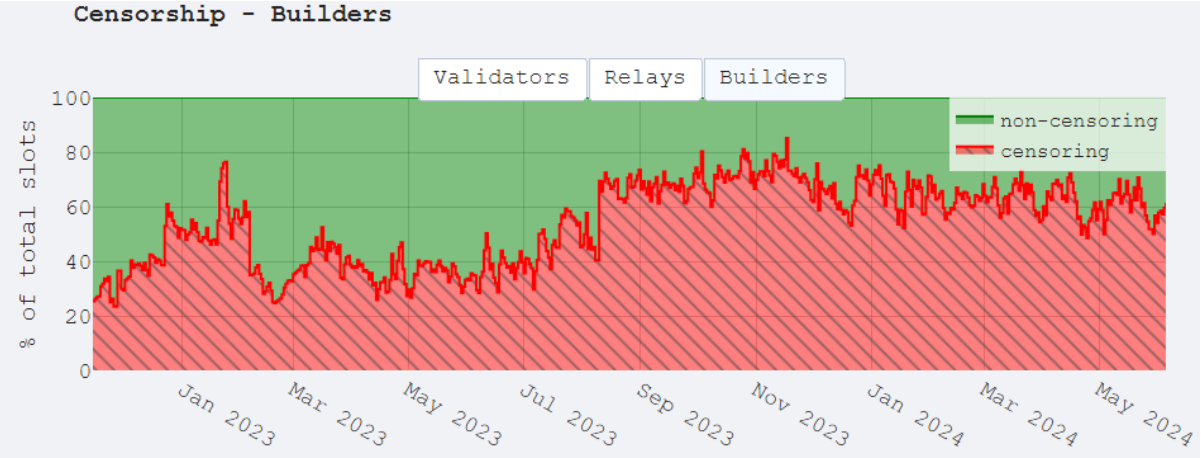
Volume is essential for dark pools to function effectively. It helps to efficiently match orders and preserve trader anonymity. The more anonymized funds there are in the pool or the more orders in the order book, the more difficult it is to link depositors and traders to their assets. This is because there are more potential depositors to try and link assets to. It is also important to consider the type of token when shielding assets. Shielding common stablecoins like USDC or DAI will offer greater anonymity than shielding unknown meme tokens with very few depositors.



MEV & Censorship Resistance

Most DEXs operating on public blockchains, by being an open, transparent ledger, allow for MEV to exist. Order details on DEXs like Uniswap or Curve are not confidential. This allows searchers and builders to rearrange transactions in bundles and blocks accordingly to extract MEV.

Privacy is good but it is a subjective matter. Tornado Cash was great at allowing people to anonymously conduct their financial activities on-chain. By it being open-source and free for anyone to use, it also had criminals using it to launder stolen funds. North Korean hacker group, Lazarus has stolen close to a billion dollars ($958 Mn) so far. OFAC (Office of Foreign Asset Control) maintains a list of specially designated nationals and blocked individuals. Malicious individuals and entities such as Lazarus and even Tornado Cash's smart contract address are on the OFAC list for non-compliance. Protocols that are not OFAC compliant face a high chance of having their transactions excluded from blocks that get added on-chain. This is because the top 5 of the 6 largest block builders are OFAC compliant. Is this a serious censorship resistance issue? Yes. It doesn't stop with Builders. Validators and relayers can also choose to omit transactions or blocks.



Source: Censorship.pics

With dark pools, order details mostly remain hidden from all third parties including validators given that ZKPs are issued for each order, eliminating the need to reveal details for order matching or even settlement. This architecture could be MEV and censorship-resistant or it would at least be the case as long as transaction work-flow remains within a dark pool's encrypted premise. In cases where public contracts are called or a shared sequencer is used, MEV-capturing opportunities may again arise.

SEC's Good Book

Whether you're operating within a protocol or as an individual user, the last thing you'd want is to see your transactions left hanging, unprocessed within blocks, risking the success of your state transition, or having the SEC come over for a tea party. These concerns became a grim reality for the founders and developers of Tornado Cash, who were arrested on money-laundering charges. The TC front-end is also illegal/defunct in many countries and is not supported by several CEXs. The TC smart contracts themselves are still operational and can be used by folks with a bit of technical know-how.

To try and avoid such situations, dark pools and other privacy-focused protocols have found ways to allow the user to maintain compliance at the user's discretion.

Panther Protocol uses the concept of zones and zone managers. A zone manager is a licensed entity that regulates a zone or a trading area by allowlisting traders and assets. Pathner Protocol supports integrations from multiple compliance providers that users or zone managers could choose from. Panther does not learn user data but allows compliance providers to process their data and attest

to the validity of their KYC statements by producing ZK proofs.

Renegade can allow each trader to choose a set of counterparties to trade with. An individual trader may just want some basic AML/sanction checks on their counterparties whereas an institution may want to have KYB/KYC checks done on their counterparties. This counterparty selection logic with compliance checks using ZKPs can be set before MPC begins.

With Penumbra, Users can demonstrate compliance off-chain using 'transaction perspectives' to disclose their activity, including the provenance of funds selectively. Similarly, with Railgun, users have "viewing keys" that allow users to view transactions and balances from X to Y block time.

Singularity works with compliance oracles who in turn work with traditional compliance service providers to KYC/KYB verify user accounts off-chain. Once verified, the user is given a ZK proof of compliance. This Proof allows their wallet to be functional with the dark pool protocol. The verification would need to be done on a recurring basis.

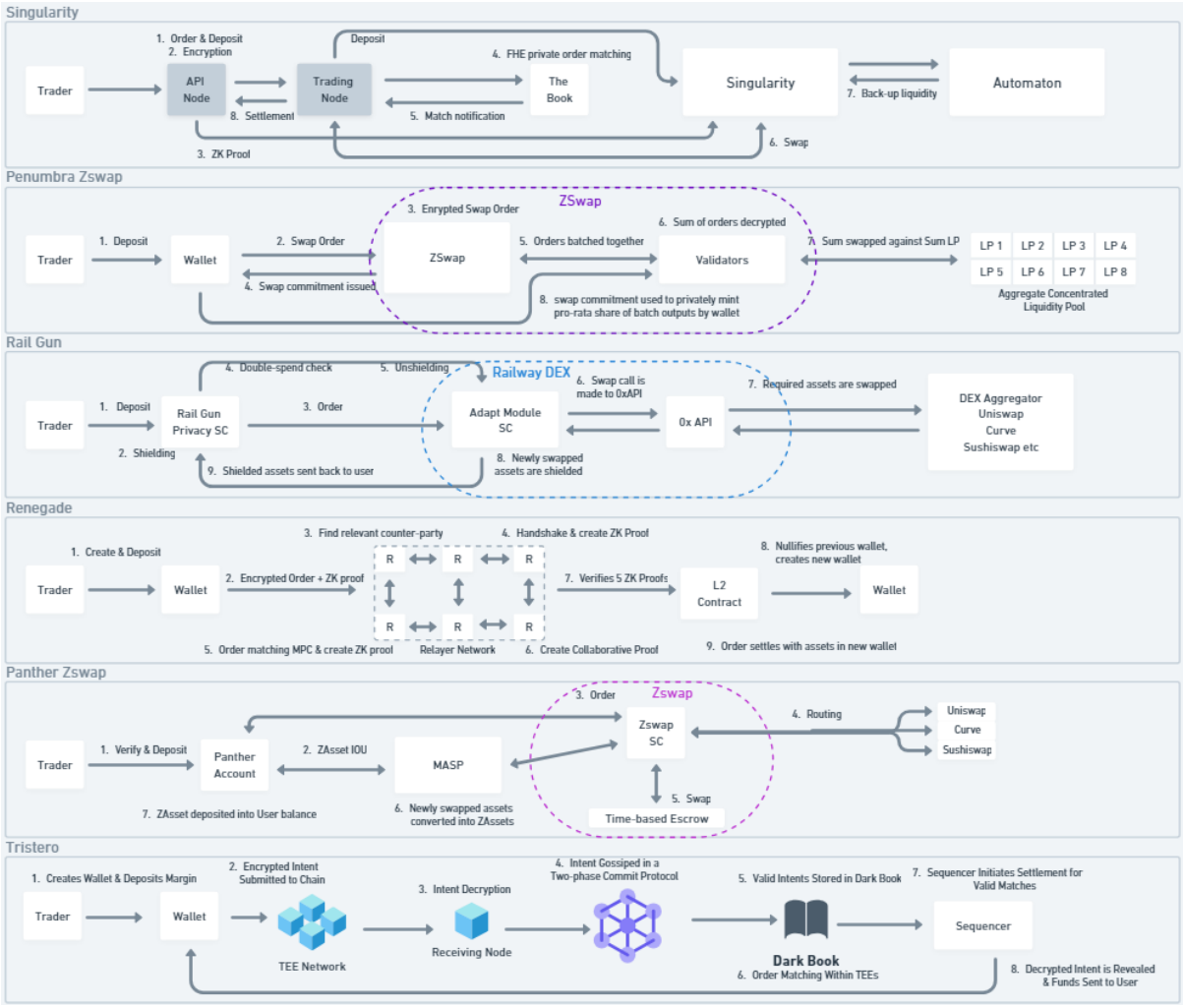
Railgun uses "Proof of Innocence", talked about in the Privacy Pools 2.0 paper, developed by Chainway. Proof of Innocence helps you prove that your transactions are legitimate without revealing any transaction details. Merkel trees act as an aggregate of all previous UTXOs (transactions, balances). With this, it is possible to determine that a particular balance was a part of a certain transaction set. But to prove that a particular balance was NOT part of a certain transaction set, a Sparse Merkle tree is needed that records NULL values. With this proof can be generated to verify that the balance was not part of a certain transaction set. In this case, Recursive SNARKs are used to prove that the chain of proofs right from the initial deposit to the eventual withdrawal was calculated accurately as proof that a user's balance was NOT part of a certain transaction set.

Lingering Thoughts

Dark pool users rely on public prices as a benchmark for their traders but the prices of assets on public exchanges may not reflect movements happening within dark pools. Price discovery was a one-sided relationship between dark pools and public exchanges until 2014. FINRA and the SEC brought into effect an initiative where dark pool trading information post settlement was to be published publicly on a security-by-security basis with a 2-4 week delay. It is

unknown if similar public disclosure standards may be applied to crypto dark pools in the future to promote better price discovery for all market participants.

Order life cycle across different privacy-preserving workflows



Pure Play Dark Pools will have to bootstrap order flow on both sides of the market in order to reach critical mass. We may see much of OTC deals move over to dark pools as they would be considerably more secure, private, and cost-efficient than OTC desks and Telegram groups. In cases where private DEXs interact with public liquidity pools or external smart contracts, running simulations on leaked information may lead to the unraveling of certain trades and traders.

A special thanks to Avi (Delphi Digital) and Owen (Sei Network) for the review and Anish Mohammed & Joris (Panther Protocol), Chris (Renegade), Sam (Tristero), Henry (Penumbra), contributors from Railgun, Loong & Jemma (Singularity) and Ian (GSR) for their feedback and insights.